Index

Note to the Reader: Throughout this index boldfaced page numbers indicate primary discussions of a topic. Italicized page numbers indicate illustrations.

A
A records
    creating, 375–376, 375
description, 363
AAAA records, 363
access control in S3, 217, 219
access control lists (ACLs), 219
access keys in IAM
description, 274
generating, 286
managing, 279–281, 280
accessibility in AMIs, 255–256, 256–257
account compromise in Amazon GuardDuty, 319–320
AccountID parameter for CloudFormation templates, 392
accounts, service control policies for, 67–68
ACLs (access control lists), 219
Action element in IAM policies, 275
actions driven by monitoring, 36
ALARM state in IAM policies, 275
alarms in CloudWatch
    description, 36
    vs. events, 37
    notifiable changes, 36
    overview, 44–45, 301–302
    Route 53 monitoring, 371
    setting up, 307–308, 308
Alias field
    failover routing policy, 367
geolocation routing policy, 368
latency routing policy, 369
multivalue answer routing policy, 370
simple routing policy, 367
weighted routing policy, 370
alias records, 364
all-at-once Elastic Beanstalk deployment, 409
All option for management events, 298
AllocationStrategy termination policy, 152
Allow Users To Change Their Own Password setting, 279
AllowedPattern method, 389
AllowedValues method, 389
AllRequests metric, 42
Amazon Athenas
    CloudTrail logs, 106
    functions, 13
Amazon Aurora
    benefits, 131
    overview, 132–133
Amazon CloudWatch. See CloudWatch
Amazon Cognito
description, 282–283
functions, 13
Amazon Elastic Block Store. See Elastic Block Storage (EBS)
Amazon Glacier
functions, 11
overview, 222–223
Amazon Glacier Deep Archive, 223
Amazon GuardDuty. See GuardDuty
Amazon Inspector
ean essentials, 320–321
overview, 316–318, 317
resources, 320
review questions, 326–329
setting up, 321–323, 322–323
summary, 320
Amazon Machine Images (AMIs)
    accessibility, 255–256, 256–257
    bastion hosts, 169
    creating, 262–263, 262
    Elastic Beanstalk, 404
    exam essentials, 261
    exercises, 261–263, 262–263
    instance stores, 242
    issues, 260
    moving between regions, 258, 259, 259
    NAT, 342
    overview, 254–255
    resources, 260–261
    review questions, 264–267
    security, 258, 263, 263
    storage, 257
    summary, 260
Amazon RDS. See Relational Database Service (RDS)
Amazon Route 53, See Route 53
Amazon Route 53 Resolver, 365
Amazon Simple Storage Service. See Simple Storage Service (S3)
Amazon Traffic Flow, 366
AmazonEC2RoleforSSM policy, 189
AMIs. See Amazon Machine Images (AMIs)
Analytics category
core services, 13
functions, 9
Anywhere option for security groups, 346
Apache, installing, 200–201, 201
API logs, 102–106, 103–105
applications, testing, 410
assessments
    Amazon Inspector, 316–318, 317
    continuous, 80
Associate With Health Check field
    failover routing policy, 368
geolocation routing policy, 368
latency routing policy, 369
multivalue answer routing policy, 370
weighted routing policy, 371
Athena
- CloudTrail logs, 106
- functions, 13
- audit trails, 83

Auto Scaling
- cooldown periods, 150–151
- EC2, 144
- exam essentials, 153–154
- exercises, 154–157, 156–157
- failures, 152
- functions, 13
- groups
  - creating, 155–157, 156–157
  - launch configurations, 148
  - overview, 143, 143
  - scaling, 145–146
- instances
  - maintenance, 146
  - termination order, 151–152
- launch configurations
  - creating, 154–155
  - overview, 147–149
- minimums, maximums, and desired capacity, 145
- overview, 142
- resources, 153
- review questions, 158–161
- scaling in and scaling out, 143–144
- strategies, 149–152
- summary, 153
- terms and concepts, 142–146, 143

Auto Scaling Group
- Only deployment for Elastic Beanstalk, 403
- automation documents, 192
- availability in 53, 215–217
- availability zones (AZs)
  - and regions, 7–8
  - VPCs, 337, 337
- Average metric in CloudWatch, 38
- AWS CLI (command-line interface)
  - Elastic Beanstalk, 414
  - moving AMIs between regions, 259
  - overview, 19
  - working with, 21–23
- AWS CloudFormation
  - See CloudFormation
- AWS CloudTrail
  - See CloudTrail
- AWS CodeBuild, 193
- AWS CodeDeploy, 193
- AWS Config
  - audit trails, 83
  - centralized configuration management, 81–82
  - vs. CloudTrail, 87
  - configuration changes
    - cloud, 80–81
    - continuous, 79–80
    - on-premises solutions, 80
    - overview, 78–79
  - configuration components, 84
  - exam essentials, 88
  - exercises, 89–95, 90–93
  - functions, 12
  - monitoring, 304–305, 309–310, 310
  - overview, 78
  - resources, 88
- review questions, 96–100
- rules, 83–87, 85
- security, 83
- summary, 87
- turning off, 95
- turning on, 94
- AWS Direct Connect
  - functions, 11
  - gateways, 318
  - VPCs, 336, 344–345
- AWS-GatherSoftwareInventory document, 195, 195
- AWS Hypervisor, 35
- AWS IAM. See Identity and Access Management (IAM)
- AWS KMS-Managed Keys (SSE-KMS), 222
- AWS Lambda events and functions
  - CloudTrail, 299, 299
  - configuration rules, 86
  - event targets, 47
  - functions, 10
- AWS Management Console
  - IAM access keys, 280
  - moving AMIs between regions, 259, 259
  - overview, 17–18, 17–18
- AWS OpsWorks, 80
- AWS Organizations
  - collections of accounts, 64
  - consolidated billing, 68–69
  - creating, 70–71
  - exam essentials, 70
  - exercises, 70–72
  - functions, 13
  - master accounts, 65
  - multiple accounts, 62–64
  - organizational units, 65–66, 66
  - overview, 62
  - review questions, 73–76
  - service control policies, 66–68, 67
  - summary, 69
  - vs. tagging, 69
- AWS Policy Generator, 277, 277
- AWS Policy Simulator, 277
- AWS SDKs (software development kits), 19
- AWS services model, 6–7, 6
- AWS Systems Manager. See Systems Manager (SSM)
- AWS systems operations overview, 5
- AWS CLI, 19
- AWS management console, 17–18, 17–18
- AWS SDKs, 19
- domains, 16
- ecosystem
  - AWS services model, 6–7, 6
  - global presence, 7–8
  - overview, 5–6, 5
- exam essentials, 21
- exercises, 21–23
- key exam resources, 20
- key principles, 14
- managed services, 8–14
- review questions, 24–27
- service level agreements, 16
- Shared Responsibility Model, 15–16, 15
- summary, 21
- support plans, 20
- technical support and online resources, 19
AWS CloudTrailFullAccess permission, 108
AWS CloudTrailReadOnlyAccess permission, 108
AWS Elastic Beanstalk FullAccess policy, 412
AWS Elastic Beanstalk ReadOnlyAccess policy, 412
AWSLogs folder, 106
AWSTemplateFormatVersion section, 385
AZs (availability zones) and regions, 7–8
VPCs, 337, 337

B

backing up instances, 128–129
Base64 function, 390–391
baselines for Patch Manager, 192
Basic support plan, 20
bastion hosts
on cloud, 172
creating, 178–181, 179–182
exam essentials, 172
overview, 169–171, 171
review questions, 183–186
summary, 172
VPCs, 338
best practices
Elastic Beanstalk security, 413
host assessments, 318
IAM, 281–282
master accounts, 65
billing, consolidating, 63–64, 68–69
block storage in EBS. See Elastic Block Storage (EBS)
blue/green Elastic Beanstalk deployments, 410
breaching setting for CloudWatch alarms, 302
broadcast IP addresses, 335
buckets. See Simple Storage Service (S3)
BucketSizeBytes metric, 42
built-in functions for CloudFormation templates, 390–391
Business support plan, 20
BytesDownloaded metric, 42
BytesUploaded metric, 42

C

CAA records, 363
cached mode for volume gateways, 225
canonical name (CNAME) records, 363
capacity in Auto Scaling, 145
categories of services, 6, 6
Center for Internet Security (CIS)
benchmarks, 318
description, 317
centralized configuration management, 81–82, 81–82
change triggers for configuration rules, 86
ChangeInCapacity parameter, 150
Chef product, 80
CIDR (Classless Inter-Domain Routing), 335
Cidr function, 390
CIS (Center for Internet Security)
benchmarks, 318
description, 317
Classless Inter-Domain Routing (CIDR), 335
CLI (command-line interface)
Elastic Beanstalk, 414
moving AMIs between regions, 259
overview, 19
working with, 21–23
ClosestToNextInstanceHour termination policy, 152
cloud, configuration in, 80–81
CloudFormation
exam essentials, 393
exercises, 394, 395
functions, 12
IaaS, 384–385
overview, 384
resources, 393
review questions, 396–399
stacks
creating, 394, 395
overview, 389–390
summary, 392–393
templates
built-in functions, 390–391
improving, 390–392
issues, 392
mappings, 391–392
overview, 385–389
CloudFront service functions, 11
CloudTrail
API logs, 102–106, 103–105
vs. AWS Config, 87
costs, 300
data events, 298 299, 299
exam essentials, 109
exercises, 109–114, 110–114
functions, 12
management events, 298
monitoring with, 106–108
overview, 102, 296–297, 297
permissions, 108
process, 105–106, 105–106
regions, trails in
applying, 298, 298
creating, 109–111
working with, 104–105
resources, 108
review questions, 115–118
summary, 108
trails
creating, 109–111, 110–111
notifications, 113–114, 114
setting up, 306–307
CloudWatch
alarms
description, 36
vs. events, 37
overview, 44–45, 301–302
Route 53, 371
setting up, 307–308, 308
Dashboard
creating, 49–51, 50–51
description, 303, 304
setting up, 308–309, 309
events, 46–47, 303
exam essentials, 48–49
exercises, 49–55, 50–55
functions, 12
CloudWatch Events (CWE) – EBS

logs, 302–303
monitoring
customizable monitoring, 34–35, 35
CVE (Common Vulnerabilities and Exposures)
description, 317
host assessments, 318
CWE (CloudWatch Events), 37, 46
Cyber Kill Chain, 319, 319

D
Dashboard in CloudWatch
creating, 49–51, 50–51
description, 303, 304
setting up, 308–309, 309
data events in CloudTrail, 298–299, 299
data protection in Elastic Beanstalk, 412
Database category
core services, 11–12
default encryption
EBS, 247
S3, 221, 228
Db2
Default termination policy for Auto Scaling instances, 152
DeleteObject function, 299
deployment
configuration management, 79
Elastic Beanstalk, 403, 409–410
description section in CloudFormation templates, 385
desired capacity in Auto Scaling, 145
Developer support plan, 20
Developer Tools functions, 9
dimensions in metrics, 38–39
Direct Connect
core services, 10
default encryption
EBS, 247
S3, 221, 228
database service. See Relational Database Service (RDS)
DatabaseConnections metric, 43
Datapoints To Alarm settings, 301–302
default encryption
EBS, 247
S3, 221, 228
Default termination policy for Auto Scaling instances, 152
DeleteObject function, 299
deployment
configurations management, 79
Elastic Beanstalk, 403, 409–410
description section in CloudFormation templates, 385
desired capacity in Auto Scaling, 145
Developer support plan, 20
Developer Tools functions, 9
dimensions in metrics, 38–39
Direct Connect
functions, 11
gateways, 318
VPCs, 336, 344–345
DiskQueueDepth metric, 43
DiskReadBytes metric, 40
DiskReadOps metric, 39
DiskWriteBytes metric, 40
DiskWriteOps metric, 39
DNSSEC (DNS Security), 363
documents in Systems Manager, 191–192
Domain Name System (DNS)
overview, 362–363
records, 363–364
Route 53, 364–366, 365
domains, 16
durability in S3, 215–217
dynamic scaling, 150
DynamoDB service functions, 12
DynamoDB2 metrics, 43–44

E
EBS. See Elastic Block Storage (EBS)
EBSByteBalance metric, 40
Elastic Container Service (ECS), 102

EC2. See Elastic Compute Cloud (EC2)

EBSWriteOps metric, 40

Elastic Beanstalk blue/green deployments, 410

CL1, 414

configuring, 410–411, 411

exam essentials, 416

exercises, 416–417, 417

functions, 10

languages, 403–404, 404

overview, 402–403

platforms

creating, 405–407, 408

overview, 403–404, 404

resources, 415–416

review questions, 418–421

security, 412–413

summary, 415

troubleshooting, 414–415

updates, 408–410

Elastic Block Storage (EBS)

block storage types, 239–241, 241

exam essentials, 245

exercises, 245–247

functions, 11

vs. instance stores, 241–242

overview, 238–239

resources, 244

review questions, 248–251

snapshots

encryption, 246–247, 246

overview, 244

summary, 244

volumes

creating, 245

encryption, 242–243, 243, 246–247, 246

metrics, 40–41

Elastic Compute Cloud (EC2)

functions, 10

instances

from AMIs, 261–262

Auto Scaling, 144, 147–148

metrics, 39–41

network assessments, 318

Session Manager, 202, 202

tags, 199

Elastic Container Service (ECS), 102

event targets, 47

functions, 10

metrics, 41

elastic load balancers (ELBs)

functions, 10

network assessments, 318

Elastic MapReduce (EMR)

functions, 13

storage, 41

elastic network interface (ENI)

interface endpoints, 343

network assessments, 318

Elastic Transcoder service functions, 13

ElasticCache service functions, 12

ELBs (elastic load balancers)

functions, 10

network assessments, 318

e-mail addresses in IAM, 274

EMR (Elastic MapReduce)

functions, 13

storage, 41

EMS-backed AMIs, 257

Enable Password Expiration setting, 279

encryption

AMIs, 258

S3, 221–222, 227–228

volumes

overview, 242–243, 243

snapshots, 246–247, 246

endpoints

Route 53 monitoring, 371

VPCs, 342–344, 353

ENI (elastic network interface)

interface endpoints, 343

network assessments, 318

Enterprise support plan, 20

evaluation

CloudWatch alarms, 301

configuration rules, 85–87

event-driven monitoring in CloudWatch, 33, 34, 36

events

CloudTrail, 298–299, 299

CloudWatch

vs. alarms, 37

components, 37

description, 303

generating, 46

rules, 46–47

targets, 47

ExactCapacity parameter in dynamic scaling, 150

F

failover

RDS, 130–131

Route 53

A records for, 375–376, 375

overview, 371–372, 371

routing policies, 367–368

Federation, 283

file gateways in S3, 225

FindInMap function, 390

FirstByteLatency metric, 42

flow logs for VPCs, 347–348

FQDNs (fully qualified domain names), 363

FreeStorageSpace metric, 43

frequency of alarm monitoring, 45

fully qualified domain names (FQDNs), 363
gateways

Direct Connect, 318
endpoints, 343–344
IGW
  bastion hosts, 170
  network assessments, 318
  VPCs, 339–340
NAT, 340–341, 341
storage, 224–225
VPCs, 344
Gemalto SafeNet tokens, 274
general-purpose SSD (gp2) volumes, 239–240
geolocation routing policy in Route 53, 368
geopproximity routing policy in Route 53, 368–369
GetAtt function, 390
GetAZs function, 390
GetObject function, 299
GetRequests metric, 42
Glacier
  functions, 11
  overview, 222–223
  global presence, 7–8
golden images, 414
groups
  Auto Scaling
    creating, 155–157, 156–157
    launch configurations, 148
    overview, 143, 143
    scaling, 145–146
  CloudWatch logs, 302–303
  IAM, 274
  security, 345–346, 346, 354
  Systems Manager, 191, 199, 200
GuardDuty
  exam essentials, 320–321
  overview, 318–320, 319
  resources, 320
  review questions, 326–329
  setting up, 323–325, 324–325
  summary, 320

H

hardware tokens in IAM, 274
health checks
  Auto Scaling, 146
  Route 53
    creating, 374–375
    overview, 371–372, 371
host assessments in Amazon Inspector, 316–318
host bits in IP addresses, 335
hosted zones, creating, 373
hub-and-spoke architecture, 168, 168
Hypervisor and CloudWatch, 35

I

IaaS (infrastructure as a service), 384–385
Identity and Access Management (IAM)
  access keys
    generating, 286
    managing, 279–281, 280
  best practices, 281–282
  building blocks
    groups, 274
    policies, 275–277, 277
    roles, 274–275, 288–289
    users, 273–274, 285
  Cognito, 282–283
  Elastic Beanstalk, 412
  exam essentials, 284–285
  exercises, 285–289, 287
  Federation, 283
  functions, 13
  Key Management Service, 283
  multiple accounts, 62–63
  overview, 272
  passwords
    managing, 278–279, 278
    policies, 288
  resources, 284
  review questions, 290–293
  roles
    creating, 90, 90–91
    permissions, 91–95, 92–93
    root accounts, 281
  service control policies, 66–68, 67
  Shared Responsibility Model, 272–273, 273
  summary, 283–284
  Systems Manager, 189
  Trusted Advisor, 282, 282
  ignore setting for CloudWatch alarms, 302
IGWs (Internet gateways)
  bastion hosts, 170
  network assessments, 318
  VPCs, 339–340
  immutable deployments for Elastic Beanstalk, 409–410
  ImportValue function, 390
  infrastructure as a service (IaaS), 384–385
  inline policies in IAM, 275
  input/output operations per second (IOPS), 238–240
  instance-backed AMIs, 257
  instance compromise in GuardDuty, 319
  instances
    from AMIs, 261–262
  Auto Scaling
    maintenance, 146
    termination order, 151–152
    backing up, 128–129
    EBS stores, 241–242
    metrics, 39–41
    NAT, 341–342, 342
    network assessments, 318
    vs. RDS, 123–125, 123–124
    scaling, 128
    security, 129
    Systems Manager, 190–191, 190
    tags, 199
  INSUFFICIENT_DATA state in CloudWatch alarms, 301
  integration in configuration management, 79
  interface endpoints, 343
  Internet gateways (IGWs)
bastion hosts, 170
network assessments, 318
VPCs, 339–340
Internet Protocol (IP), 334
Internet Small Computer Systems Interface (iSCSI), 225
interregion peering, 169
IOPS (input/output operations per second), 238–240
IP addresses
bastion hosts, 170
CIDR, 335
DNS, 362–366, 365
failover situations, 131
VPCs, 336
endpoints, 342–344
IGWs, 339–340
NAT, 340–342, 341–342
route tables, 338–339, 338–339
subnets, 337–338, 337
IP (Internet Protocol), 334
iSCSI (Internet Small Computer Systems Interface), 225
IsMultiRegionTrail setting, 298

J

JavaScript Object Notation (JSON)
bucket policies, 218
CloudFormation templates, 385, 392
documents, 191
event targets, 47
user policies, 218
Join function, 390
jumbo frames in VPN peering, 169

K

Key Management Service (KMS)
EBS, 243, 243
IAM, 283
Parameter Store, 193
keys
IAM
access key rotation, 280–281
key pairs, 274
object, 213
Kinesis service functions, 13

L

Lambda events and functions
CloudTrail, 299, 299
configuration rules, 86
event targets, 47
functions, 10
languages for Elastic Beanstalk, 403–404, 404
latency routing policy in Route 53, 369
launch configurations in Auto Scaling
creating, 154–155
overview, 147–149
launch permissions in AMIs, 258, 263, 263
least privilege concept in IAM, 274
license key parameters, 201–202
Lifecycle Management in S3, 223, 231
lifecycle policies in S3, 230–231, 231
line metrics, 51–52, 52–53
Linux bastion hosts, 170, 172
Load Balancer and Auto Scaling Group deployment for
Elastic Beanstalk, 403
load balancers
functions, 10
network assessments, 318
VPCs, 337
Location field in geolocation routing policy, 368
logs
bastion hosts, 170
CloudTrail
trails, 102–106, 103–105
viewing, 106–107, 112, 112–113
CloudWatch, 302–303
Elastic Beanstalk, 412
and reporting. See reporting and logging
VPCs, 347–348
low levels events, 37

M

mail exchange (MX) records, 363
managed instances in Systems Manager, 190–191, 190
managed policies in IAM, 275
managed services, 8–14
management events in CloudTrail, 298
Management Tools category
core services, 12–13
functions, 9
manual scaling, 149
mappings in CloudFormation templates, 386–387, 391–392
masks in CIDR, 335, 335
master accounts, 65
Maximum metric in CloudWatch, 38
maximums in Auto Scaling, 145
MaxLength method, 389
MaxValue method, 389
Media Services category
core services, 13
functions, 9
MemoryReservation metric, 41
MemoryUtilization metric, 41
metadata
CloudFormation templates, 386
in configuration, 85
metrics in CloudWatch
description, 36
dimensions, 38–39
EC2, 39–41
line, 51–52, 52–53
purpose, 33
storage, 41–44
MFA (Multi-Factor Authentication)
bastion hosts, 170
IAM
description, 274
enabling, 286–287, 287
Migration category
  core services, 12
  functions, 9
Minimum metric in CloudWatch, 38
Minimum Password Length setting, 279
minimums in Auto Scaling, 145
MinLength method, 389
MinValue method, 389
missing setting for CloudWatch alarms, 302
monitoring. See also reporting and logging
  actions driven by, 36
  CloudTrail, 106–108
  compute, 39–41
  configuration management, 79
  customizable, 34–35, 35
  Elastic Beanstalk, 412
  event-driven, 33, 34
    events, 46–47
    overview, 32–33
    storage, 41–44
moving AMLs between regions, 258–259, 259
multi-AZ configurations in RDS, 129–130, 130
Multi-Factor Authentication (MFA)
  bastion hosts, 170
  IAM
description, 274
  enabling, 286–287, 287
multiple accounts, managing, 62–64
multivalue answer routing policy in Route 53, 369–370
MX (mail exchange) records, 363
My IP option for security groups, 346

N
NACLs. See network access control lists (NACLs)
Name Authority Pointer (NAPTR) records, 363
Name field
  failover routing policy, 367
  geolocation routing policy, 368
  latency routing policy, 369
  multivalue answer routing policy, 370
  simple routing policy, 367
  weighted routing policy, 370
Name Server (NS) records, 363
names for regions, 8
namespaces in CloudWatch, 37–38
NAPTR (Name Authority Pointer) records, 363
NAT. See network address translation (NAT)
network access control lists (NACLs)
  network assessments, 318
VPCs
  creating, 354–355
  overview, 346–347, 347
  traffic flow, 167
network address translation (NAT)
  bastion hosts, 170
description, 334–335
  gateways, 340–341, 341
  instances, 341–342, 342
network assessments in Amazon Inspector, 316, 318
network bits in IP addresses, 335
Network File System (NFS) storage gateways, 225
network interfaces (ENIs)
  interface endpoints, 343
  network assessments, 318
NetworkIn metric, 40
Networking & Content Delivery category
  core services, 10–11
  functions, 9
NetworkOut metric, 40
NetworkPacketsIn metric, 40
NetworkPacketsOut metric, 40
networks for VPCs. See virtual private clouds (VPCs)
NewestInstance termination policy, 152
NFS (Network File System) storage gateways, 225
notBreaching setting for CloudWatch alarms, 302
notifiable changes, alarms for, 36
NotificationARNs parameter for CloudFormation templates, 392
notifications for trails, 113–114, 114
NoValue parameter for CloudFormation templates, 392
NS (Name Server) records, 363
NumberOfObjects metric, 42

O
object storage in S3, 212–215, 213
OK state in CloudWatch alarms, 301
OldestInstance termination policy, 152
OldestLaunchConfiguration termination policy, 152
OldestLaunchTemplate termination policy, 152
on-premises configuration change solutions, 80
one-time PINs (OTPs), 274
online resources, 19
organizational units (OUs), 65–66, 66
OTPs (one-time PINs), 274
Outputs section
  CloudFormation stacks, 390
  CloudFormation templates, 388–389

P
Packer tool, 405–406
Parameter Store, 192–194
parameters
  CloudFormation stacks, 389
  CloudFormation templates, 386, 392
  license keys, 201–202
  RDS, 125–126, 126
Partition parameter for CloudFormation templates, 392
Password Expiration Requires Administrator Reset setting, 279
passwords in IAM
description, 274
  policies
    creating, 288
    managing, 278–279, 278
Patch Manager
  configuring, 203–204, 203
  overview, 192
path-style URLs for S3 buckets, 214
peering, VPC. See virtual private clouds (VPCs)
PercentChangeInCapacity parameter, 150
percentile metric in CloudWatch, 38
periodic triggers for configuration rules, 86
periods for CloudWatch alarms, 301
permissions
AMI launch, 258, 263, 263
CloudTrail, 108
S3 buckets, 91–93, 92–93
persistent storage, 239
platform archives in Elastic Beanstalk, 405
platform definition files in Elastic Beanstalk, 405
platforms in Elastic Beanstalk
creating, 405–407, 408
overview, 403–404, 404
pointer (PTR) records, 364
policies
dynamic scaling, 150
IAM
overview, 275–277
passwords, 278–279, 278, 288
service control, 66–68, 67
Route 53 routing, 366–371
S3, 218–219, 229–231, 231
policy documents in Systems Manager, 192
prebuilt rules in configuration, 85–86
Prevent Password Reuse setting, 279
Principal element in IAM policies, 275
private AMIs, 255
private DNS, 366
private subnets, 337
provisioned IOPS SSD (io1) volumes, 239–240
ProvisionedReadCapacityUnits metric, 44
ProvisionedWriteCapacityUnits metric, 44
pseudo parameters in CloudFormation templates, 392
PTR (pointer) records, 364
public access settings in S3, 219–220, 220
public AMIs, 255
public subnets, 337
Puppet product, 80
PutObject function, 299

Relational Database Service (RDS)
core services, 12
database configuration and parameter groups, 125–126, 126
database creation, 122–128, 123–124, 126–127
exam essentials, 134–135
failover to secondary instances, 130–131
functions, 11
vs. instances, 123–125, 123–124
key features, 128–129
metrics, 42–43
multi-AZ configurations, 129–130, 130
overview, 122
read replicas, 131–132
resources, 134
review questions, 136–140
scalability, 127–128, 128
summary, 133–134
supported database engines, 125
relationships component in configuration, 85
Remote Desktop Protocol (RDP)
key pairs for, 274
security groups, 345
ReplicaLag metric, 43
replicas
Amazon Aurora, 133
RDS, 131–132
ReplicationLatency metric, 44
reporting and logging
AWS Config, 304–305
CloudTrail, 296–300, 297–299
CloudWatch, 300–303, 300, 304
exam essentials, 306
exercises, 306–310, 308–310
overview, 296
resources, 305–306
review questions, 311–314
summary, 305
Require At Least One Lowercase Letter setting, 279
Require At Least One Non-alphanumeric Character setting, 279
Require At Least One Number setting, 279
Require At Least One Uppercase Letter setting, 279
reserved IP addresses, 335
resilience in Elastic Beanstalk, 413
resource attributes component in configuration, 85
Resource element in IAM policies, 275
resource groups in Systems Manager, 191, 199, 200
Resources section in CloudFormation templates, 388
responding to alarms, 45
roles
IAM
creating, 90, 90–91, 288–289
overview, 274–275
permissions, 91–93, 92–93
Systems Manager, 197–198, 198
rolling deployments in Elastic Beanstalk, 409
rolling with additional batches deployment in Elastic Beanstalk, 409
root accounts, protecting, 281
Route 53
Amazon Traffic Flow, 366
DNS, 362–366, 365
exam essentials, 373
exercises, 373–376, 375
functions, 11
health checks and failover, 371–372, 371

R

RDP (Remote Desktop Protocol)
key pairs for, 274
security groups, 345
RDS. See Relational Database Service (RDS)
reachability rules in Amazon Inspector, 318
Read-only option for management events, 298
read replicas, 131–132
ReadIOPS metric, 43
ReadLatency metric, 43
reconnaissance activities in Amazon GuardDuty, 319
records, DNS, 363–364
RedShift
functions, 12
storage, 41
Region field in latency routing policy, 369
Region parameter for CloudFormation templates, 392
regions
and availability zones, 7–8
CloudTrail, 298, 298
moving AMIs between, 258, 259, 259
read replicas, 132
S3 buckets, 214–215
trails, 104–105, 109–111, 110–111
VPN peering, 169
hosted zones, 373
overview, 362
resources, 372
review questions, 377–380
routing policies, 366–371
summary, 372
route tables
network assessments, 318
VPCs, 338–339, 338–339
routing policies in Route 53
failover, 367–368
golocation, 368
geoproximity, 368–369
latency, 369
multivalue answer, 369–370
overview, 366
simple, 366–367
weighted, 370–371
rules
Amazon Inspector, 318
AWS Config, 304, 309–310, 310
configuration, 83–87, 85
events, 37, 46–47
security groups, 345–346
Run command in Systems Manager, 192, 200–201, 201
Runtime Behavior Analysis, 318

S
S3. See Simple Storage Service (S3)
S3 Intelligent-Tiering, 216
S3 One Zone-IA, 217
S3 Standard, 216
S3 Standard-Infrequent Access (IA), 216–217
S3–Managed Keys (SSE-S3), 221
SampleCount metric in CloudWatch, 38
scaling and scalability
Amazon Aurora, 133
auto. See Auto Scaling
RDS, 127–128, 128
scheduled scaling, 149–150
SCPs (service control policies)
applying, 66–67, 68, 71–72
creating, 67–68
defining, 71–72
SDKs (software development kits), 19
secondary instances, failover to, 130–131
Secure Shell (SSH)
bastion hosts, 170
key pairs for, 274
security groups, 345
security
accounts, 281–282
Amazon Inspector, 316–318, 317
AMIs, 258, 263, 263
configuration as, 83
Elastic Beanstalk, 412–413
GuardDuty, 318–320, 319
IAM. See Identity and Access Management (IAM) instances, 129
S3
access control, 217
access control lists, 219
encryption, 221–222
policies, 218–219
public access settings, 219 220, 220
versioning, 220–221
VPCs, 345–347, 346–347
Security Assertion Markup Language (SAML), 282
Security Best Practices rules package, 318
Security, Identity, & Compliance category
core services, 13
functions, 9
Select function, 390
Sender Policy Framework (SPF) records, 364
Server Message Block (SMB), 225
Server Migration service functions, 12
service control policies (SCPs)
applying, 66–67, 68, 71–72
creating, 67–68
defining, 71–72
service level agreements (SLAs)
availability, 216
services, 16
Service (SRV) records, 364
Session Initiation Protocol (SIP), 363
Session Manager
EC2 instances, 202, 202
overview, 194–195, 194
Set ID field
failover routing policy, 368
golocation routing policy, 368
latency routing policy, 369
multivalue answer routing policy, 370
weighted routing policy, 371
setting off alarms, 45
shared AMIs, 255
Shared Responsibility Model
IAM, 272–273, 273
overview, 15–16, 15
Sid element in IAM policies, 275
Simple Notification Service (SNS)
configuration changes, 89
event topics, 47
trail connections, 107
Simple Queue Service (SQS) queues, 47
simple routing policy in Route 53, 366–367
Simple Storage Service (S3)
Amazon Glacier, 222–223
availability and durability, 215–217
buckets
CLI, 22–23
CloudTrail, 105–108
configuration information, 89
creating, 23, 89, 227, 227
managing, 18, 18
metrics, 42
object storage, 213–215, 213
permissions, 91–93, 92–93
policies, 218–219, 229–230
regions, 214–215
security, 217–223, 220
exam essentials, 226
exercises, 226–231, 227–229, 231
functions, 11
Lifecycle Management, 223, 231
metrics, 42
object storage, 212–215, 213
overview, 212
resources, 225–226
<table>
<thead>
<tr>
<th>Subnet</th>
<th>Network Assessments, 318</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPCs</td>
<td>Creating, 352–353</td>
</tr>
<tr>
<td></td>
<td>Overview, 337–38, 337</td>
</tr>
<tr>
<td>Sum Metric in CloudWatch, 38</td>
<td></td>
</tr>
<tr>
<td>Support Plans, 20</td>
<td></td>
</tr>
<tr>
<td>Systems Manager (SSM)</td>
<td></td>
</tr>
<tr>
<td>Apache Installation, 200–201, 201</td>
<td></td>
</tr>
<tr>
<td>Communication, 189–190</td>
<td></td>
</tr>
<tr>
<td>Documents, 191–192</td>
<td></td>
</tr>
<tr>
<td>Exam Essentials, 197</td>
<td></td>
</tr>
<tr>
<td>Exercises, 197–204, 198, 200–204</td>
<td></td>
</tr>
<tr>
<td>License Key Parameters, 201–202</td>
<td></td>
</tr>
<tr>
<td>Managed Instances, 190–191, 190</td>
<td></td>
</tr>
<tr>
<td>Overview, 188, 189</td>
<td></td>
</tr>
<tr>
<td>Parameter Store, 192–194</td>
<td></td>
</tr>
<tr>
<td>Patch Manager</td>
<td></td>
</tr>
<tr>
<td>Configuring, 203–204, 203</td>
<td></td>
</tr>
<tr>
<td>Overview, 192</td>
<td></td>
</tr>
<tr>
<td>Resource Groups, 191, 199, 200</td>
<td></td>
</tr>
<tr>
<td>Resources, 196</td>
<td></td>
</tr>
<tr>
<td>Review Questions, 205–208</td>
<td></td>
</tr>
<tr>
<td>Role Creation, 197–198, 198</td>
<td></td>
</tr>
<tr>
<td>Run Command, 192, 200–201, 201</td>
<td></td>
</tr>
<tr>
<td>Session Manager, 194–195, 194</td>
<td></td>
</tr>
<tr>
<td>State Manager, 195–196, 195</td>
<td></td>
</tr>
<tr>
<td>Summary, 196</td>
<td></td>
</tr>
</tbody>
</table>

**T**

<table>
<thead>
<tr>
<th>Tags</th>
<th>VS. AWS Organizations, 69</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EC2 Instances, 199</td>
</tr>
<tr>
<td></td>
<td>Resource Groups, 199, 200</td>
</tr>
<tr>
<td></td>
<td>Tape Gateways in S3, 225</td>
</tr>
<tr>
<td></td>
<td>Target Tracking Scaling, 150</td>
</tr>
<tr>
<td></td>
<td>Targets for Events, 37, 47</td>
</tr>
<tr>
<td></td>
<td>TCP (Transmission Control Protocol), 363</td>
</tr>
<tr>
<td></td>
<td>Technical Support, 19–20</td>
</tr>
<tr>
<td></td>
<td>Templates</td>
</tr>
<tr>
<td></td>
<td>Amazon Inspector, 316–318</td>
</tr>
<tr>
<td></td>
<td>Auto Scaling Launch Configurations, 148–149</td>
</tr>
<tr>
<td></td>
<td>CloudFormation</td>
</tr>
<tr>
<td></td>
<td>Built-in Functions, 390–391</td>
</tr>
<tr>
<td></td>
<td>Improving, 390–392</td>
</tr>
<tr>
<td></td>
<td>Issues, 392</td>
</tr>
<tr>
<td></td>
<td>Mappings, 391–392</td>
</tr>
<tr>
<td></td>
<td>Sections, 385–389</td>
</tr>
<tr>
<td></td>
<td>Testing Applications, 410</td>
</tr>
<tr>
<td></td>
<td>Text (TXT) Records, 364</td>
</tr>
<tr>
<td></td>
<td>Text Widgets, 54–55, 55</td>
</tr>
<tr>
<td></td>
<td>Thresholds for Alarms, 45</td>
</tr>
<tr>
<td></td>
<td>Throughput-Optimized HDD (ST1) Volumes, 240</td>
</tr>
<tr>
<td></td>
<td>Time to Live Field. See TTL (Time to Live) Field Tokens in IAM, 274</td>
</tr>
<tr>
<td></td>
<td>Top-Level Domains (TLDs), 362–363</td>
</tr>
<tr>
<td></td>
<td>TotalRequestLatency Metric, 42</td>
</tr>
<tr>
<td></td>
<td>Trails. See CloudTrail</td>
</tr>
<tr>
<td></td>
<td>Transform Function, 390</td>
</tr>
<tr>
<td></td>
<td>Transforms in CloudFormation Templates, 388</td>
</tr>
</tbody>
</table>

**SSH**

<table>
<thead>
<tr>
<th>Secure Shell</th>
<th>Bastion Hosts, 170</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Key Pairs for, 274</td>
</tr>
<tr>
<td></td>
<td>Security Groups, 345</td>
</tr>
</tbody>
</table>

**SIP (Session Initiation Protocol)**, 363

**SLA (Service Level Agreement)**, 275

**SOA (Start of Authority)** records, 364

**Stacks** in CloudFormation

| Creating, 394, 395 |
|                   |
|ourtuts, 390       |
| Parameters, 389    |
| Templates, 385    |

**Start of Authority (SOA)** records, 364

**State Manager**, 195–196, 195

**Statement Element in IAM Policies**, 275

**Statistics in Metrics**, 38–39

<table>
<thead>
<tr>
<th>Step Scaling Policies, 150</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage</td>
</tr>
<tr>
<td>AMI's, 257</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>EBS. See Elastic Block Storage (EBS) Monitoring, 41–44</th>
</tr>
</thead>
<tbody>
<tr>
<td>S3. See Simple Storage Service (S3)</td>
</tr>
<tr>
<td>Storage Category</td>
</tr>
<tr>
<td>Core Services, 11</td>
</tr>
<tr>
<td>Functions, 9</td>
</tr>
</tbody>
</table>

| Storage Gateway Service Functions, 11 |
|                                      |
| Stored Mode for Volume Gateways, 225  |
| Streams, CloudWatch Logs, 302–303    |
| Sub Function, 390                     |
| Sublocation Field in Geolocation Routing Policy, 368  |
| Subnet Masks in CIDR, 335, 335        |

**SSO (Single Sign-On)**, 188

**SSM Agent**, 188

**SSO (Single Sign-On)**, 283

**StackId Parameter for CloudFormation Templates, 392**

**StackName Parameter for CloudFormation Templates, 392**

**T**

**Technical Support**, 19–20

**Templates**

<table>
<thead>
<tr>
<th>Amazon Inspector, 316–318</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Scaling Launch Configurations, 148–149</td>
</tr>
<tr>
<td>CloudFormation</td>
</tr>
<tr>
<td>Built-in Functions, 390–391</td>
</tr>
<tr>
<td>Improving, 390–392</td>
</tr>
<tr>
<td>Issues, 392</td>
</tr>
<tr>
<td>Mappings, 391–392</td>
</tr>
<tr>
<td>Sections, 385–389</td>
</tr>
<tr>
<td>Testing Applications, 410</td>
</tr>
<tr>
<td>Text (TXT) Records, 364</td>
</tr>
<tr>
<td>Text Widgets, 54–55, 55</td>
</tr>
<tr>
<td>Thresholds for Alarms, 45</td>
</tr>
<tr>
<td>Throughput-Optimized HDD (ST1) Volumes, 240</td>
</tr>
<tr>
<td>Time to Live Field. See TTL (Time to Live) Field Tokens in IAM, 274</td>
</tr>
<tr>
<td>Top-Level Domains (TLDs), 362–363</td>
</tr>
<tr>
<td>TotalRequestLatency Metric, 42</td>
</tr>
<tr>
<td>Trails. See CloudTrail</td>
</tr>
<tr>
<td>Transform Function, 390</td>
</tr>
<tr>
<td>Transforms in CloudFormation Templates, 388</td>
</tr>
</tbody>
</table>

**Transmission Control Protocol (TCP)**, 363
triggers
  CloudWatch alarms, 36
  configuration rules, 86–87
troubleshooting
  Elastic Beanstalk, 414–415
  VPCs, 347–348
Trust Advisor
  functions, 13
  IAM, 282, 288
TTL (Time to Live) field
  failover routing policy, 367
  geolocation routing policy, 368
  latency routing policy, 369
  multivalue answer routing policy, 370
  simple routing policy, 367
  weighted routing policy, 371
TXT (text) records, 364
Type field
  failover routing policy, 367
  geolocation routing policy, 368
  latency routing policy, 369
  multivalue answer routing policy, 370
  simple routing policy, 367
  weighted routing policy, 370

U
UDP (User Datagram Protocol), 363
  unified CloudWatch agent, 303
updates for Elastic Beanstalk, 408–410
URLs for S3 buckets, 214–215
URLSuffix parameter for CloudFormation templates, 392
User Datagram Protocol (UDP), 363
user policies in S3, 218
usernames in IAM, 274
users
  IAM
    creating, 285
    overview, 273–274
    management consolidation, 63

V
Value field
  failover routing policy, 367
  geolocation routing policy, 368
  latency routing policy, 369
  multivalue answer routing policy, 370
  simple routing policy, 367
  weighted routing policy, 371
Version element in IAM policies, 275
versioning in S3, 220–221, 228, 229
viewing CloudTrail logs, 106–107, 112, 112–113
virtual-hosted URLs for S3 buckets, 214
virtual private clouds (VPCs)
  connections, 344–345
  creating, 351–355, 352
  endpoints, 342–344, 353
  exam essentials, 350–351
exercises, 351–355, 352
flow logs, 347–348
functions, 10
IGWs, 339–340
NAT, 340–342, 341–342
network assessments, 318
networking overview, 334–335, 335
overview, 336
peering
  connections, 173–177, 173–177
  exam essentials, 172
  hub-and-spoke architecture, 168, 168
  interregion, 169
  overview, 166–167, 167
  resources, 172
  review questions, 183–186
  summary, 171–172
resources, 349–350
review questions, 356–359
route tables, 338–339, 338–339
security, 345–347, 346–347
subnets
  creating, 352–353
  overview, 337–338, 337
  summary, 348–349
troubleshooting, 347–348
virtual private gateways (VPGs)
  network assessments, 318
  VPCs, 344
virtual private network (VPN) connections, 336, 344
virtualization platform, 5
volumes
  Amazon Aurora, 133
  creating, 245
  encryption
    overview, 242–243, 243
  snapshots, 246–247, 246
metrics, 40–41
S3 gateways, 225
VPC Wizard, 336
VPCs. See virtual private clouds (VPCs)
VPGs (virtual private gateways)
  network assessments, 318
  VPCs, 344
VPN (virtual private network) connections, 336, 344
vulnerability analysis in Elastic Beanstalk, 413

W
weighted routing policy in Route 53, 370
  371
Write-only option for management events, 298
writing configuration rules, 86

Y
YAML Ain’t Markup Language (YAML)
  CloudFormation templates, 383
documents, 191
YubiKeys tokens, 274